UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/518,664	03/03/2000	Cameron Mashayekhi	112024-0054	6178

21186 7590 02/23/2004

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
ZIA, MOSSADEQ	

ART UNIT	PAPER NUMBER
2134	9

DATE MAILED: 02/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/518,664	Applicant(s) MASHAYEKHI, CAMERON	
	Examiner Mossadeq Zia	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 March 2000*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 5,818,936 Mashayekhi et al in view of Patent No. 5,784,566, Viavant et al.

3. In regards to **amended** claim 1, Mashayekhi discloses an authentication system suitable for automatically providing authentication to a user at a client node, the user providing a user secret and requesting access to network resources resident at one or more server nodes in a distributed network system, said authentication system:

a local application program interface for receiving the user secret, said local application program interface (workstation API) in communication with a requested network resource (applications, Mashayekhi, col. 7, line 46-48) and the client node (workstation, Mashayekhi, fig. 2, label 210);

a cryptography service node (Key Generator) (Mashayekhi, fig. 2, label 222) including means for providing a common key (private key) and algorithm (Mashayekhi, col. 5, 44-46, col. 8, line 7-8), and means for providing a client/server session key or "secure transfer" and algorithm (Mashayekhi, col. 5, line 61-63, col. 7, line 32-33, col. 8, line 8-10); and

an authentication database in communication with said local application program interface(fig.2, label 210, 240) and with said cryptography service node (Mashayekhi, fig. 2, label 222), said authentication database (Mashayekhi, fig. 2, label 204) including

an authentication secret (application secret) associated with the user (Mashayekhi, col. 5, line 62-63);

means for encrypting said authentication secret (application secret) using said common key (private key) and algorithm (Mashayekhi, col. 6, line 43, 45-47, 54-59),

Mashayekhi et al, shows that the common keys are transferred securely between client/server nodes (Mashayekhi, col. 8, line 7-9, fig. 2, label 207), but fails to show the means to encrypt the common key using the client/server session key and algorithm.

However, Viavant, et al, teaches that encryption is a type of security service by which communication over a network are encoded to help ensure privacy of sensitive data (common key) (Viavant, col. 1, line 38-40, fig. 11), and that the encryption key (session key, fig. 12, label 234) should only be known to the sender and receiver (client/server) (Viavant, col. 1, line 42-43), where algorithms such as stream cipher RC4, developed by RSA Data security, Inc., is widely used as a method for high speed encryption (Viavant, col. 1, line 45-46) to encrypt network data.

wherein the local application program interface sends an encrypted authentication secret, an encrypted common key, and the session key to the client node for use with the requested network resource (encoded, Mashayekhi, col. 7, line 32-33).

4. In regards to amended claim 9, Mashayekhi discloses a method for automatically authenticating a user at a network client node in a distributed network system in response to a

user request for access to network resources resident in one or more server nodes, said authentication method comprising the steps of:

providing a network resource identifier (Mashayekhi, col. 6, line 29, 40-42), a network resource policy (Mashayekhi, col. 6, line 28), and an authentication secret to an authentication database (user object, Mashayekhi, fig. 2, label 202, col. 6, line 25), said network resource identifier associated with the requested network resource (Mashayekhi, fig. 2, 236, col. 7, line 15);

retrieving said authentication secret in response to said user request (Mashayekhi, fig. 4a), said authentication secret (application secret) associated with the user (user's identity, Mashayekhi, col. 7, line 25-27) and with said network resource identifier (application ID, Mashayekhi, fig. 4a, block 410);

encrypting said authentication secret (encrypted data) with a common key (private key) and algorithm (Mashayekhi, col. 10, line 30-32);

Mashayekhi et al, shows that the common keys are transferred securely between client/server nodes (Mashayekhi, col. 8, line 7-9, fig. 2, label 207), but fails to show the means to encrypt the common key using the client/server session key and algorithm.

However, Viavant, et al, teaches that encryption is a type of security service by which communication over a network are encoded to help ensure privacy of sensitive data (common key) (Viavant, col. 1, line 38-40, fig. 11), and that the encryption key (session key, fig. 12, label 234) should only be known to the sender and receiver (client/server) (Viavant, col. 1, line 42-43), where algorithms such as stream cipher RC4, developed by RSA Data security, Inc., is widely used as a method for high speed encryption (Viavant, col. 1, line 45-46) to encrypt network data.

sending said encrypted authentication secret (encrypted data) and said encrypted common key (private key) to the client node (workstation node, Mashayekhi, col. 7, line 40-41, fig. 2, label 210).

5. Regarding claim 15, Mashayekhi discloses a method for authenticating a client to a nertwork resource, comprising:

receiving a client request for a network resource (Mashayekhi,col. 7, line 27-28);

authenticating the client and creating a secure session (Mashayekhi, col. 3, line 60-62, col. 5, line 47-49);

creating an authentication secret for access to the network resource (register a user, Mashayekhi, col. 5, line 42-43);

encrypting the authentication secret within a common key (Mashayekhi, col. 10, line 30-34);

encrypting the common key with an a session key associated with a secure session (Mashayekhi, col. 10, line 30-34); and

Mashayekhi et al, shows that the common keys are transferred securely between client/server nodes (Mashayekhi, col. 8, line 7-9, fig. 2, label 207), but fails to show encrypting the common key with an a session key associated with a secure session.

However, Viavant, et al, teaches that encryption is a type of security service by which communication over a network are encoded to help ensure privacy of sensitive data (common key) (Viavant, col. 1, line 38-40, fig. 11), and that the encryption key (session key, fig. 12, label 234) should only be known to the sender and receiver (client/server) (Viavant, col. 1, line 42-43),

where algorithms such as stream cipher RC4, developed by RSA Data security, Inc., is widely used as a method for high speed encryption (Viavant, col. 1, line 45-46) to encrypt network data.

transmitting to client the encrypted common key, the encrypted authentication secret, and the session key for use in accessing the network resource (Mashayekhi, col. 7, line 40-41, fig. 2, label 210).

6. Regarding claim 16, Mashayekhi discloses claim 15 above, but fails to further disclose determining a strongest encryption and decryption algorithm supported by the client when encrypting the authentication secret within the common key (Viavant, col. 3, line 25-27).

7. Regarding claim 17, Mashayekhi and Viavant et al discloses claim 15 above, and further disclose receiving, by the network resource, a decryption version of the authentication secret from the client and authenticating the client for access to the network resource based on the decrypted authentication secret (Mashayekhi, col. 7, line 46-48).

8. Regarding claim 18, Mashayekhi and Viavant at el discloses claim 15 above, and further disclose associating policies with the authentication secret, wherein the policies define access rights to the client to the network resource (Mashayekhi, col. 6, line 49-50).

9. Regarding claim 20, Mashayekhi and Viavant et al discloses claim 15 above, and further disclose associating the authentication secret with the client and the network resource and housing the association in a secret store for additional secure session established by the client (keychains, Mashayekhi, col. 6, line 43-45).

In regards to claim 8, 13, Mashayekhi and Viavant et al discloses claim 1 above, and further disclose that common key comprises a symmetric key (e.g. Menezes et al defines DES is a well known symmetric key cipher algorithm, Viavant, col. 5, line 35-39).

10. Regarding claim 19, Mashayekhi and Viavant et al discloses claim 15 above, and further disclose negotiating the client encryption and decrytption algorithms for use in encrypting the authentication secret and the common key (Viavant, col. 5, line 35-39).

Response to Amendment

11. Applicant's arguments filed on page 6-7, have been fully considered but they are not persuasive. Applicant states on page 6, paragraph 4 that authentication secret is not taught in the reference provided. This examiner respectfully disagrees. Based on the revised rejection above, Mashayekhi shows user identity and application secret to the particular application program for it to perform its authentication.

Regarding session key and the common key, Mashayekhi utilizes public/private key pair whereby this examiner interpreted the private key as the common key, and Viavant teaches the session key (Viavant, col. 11, line 30,fig. 12) whereby a shared secret must be established for the exchange controller to insure secure transfer of data.

In regards to applicant argument about application secrets is not sent to a user's machine, e.g., the client. This examiner respectfully disagrees. The workstation APIs (214) holding the encrypted data clearly resides on the workstation node (210) from within which the user interacts (Mashayekhi, fig. 2, 214, 210).

Thus, this examiner maintains the rejections to claim 1-14, and in addition rejects the newly added claims 15-20.

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
...OGY CENTER 2100

Mossadeq Zia
Examiner
Art Unit 2134

mz
2/19/04